DEPARTMENT OF THE ARMY
U.S. ARMY MANEUVER SUPPORT CENTER AND FORT LEONARD WOOD
320 MANSCEN LOOP STE 316
FORT LEONARD WOOD, MISSOURI 65473-8929

REPLY TO
ATTENTION OF

ATZT-IM (25)

09 SEP 2002

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Command Policy #43-02, Portable Electronic Devices

1. References.

a. DoDD 5200.40, Defense Information Technology Security Certification and Accreditation Process (DITSCAP).

b. DoDD 5200.28, Security Requirements for Automated Information Systems.

c. Federal Information Processing Standards FIPS 140-1.

d. Federal Information Processing Standards FIPS 140-2.

e. Assistant Secretary of Defense (ASD) Memorandum, DoD Public Key Infrastructure (PKI), August 12, 2000.

f. HQDA Ltr 25-02-1, U.S. Army Wireless Local Area (LAN) and wireless Portable.

g. Electronic Devices (PED) Policy, 15 April 2002.

h. AR 380-19, Information Systems Security.

i. AR 380-53, Information Systems Security Monitoring.

j. TRADOC Regulation 25-70, Network Services.

k. TRADOC Memorandum, Use of Information Systems, dtd 5 June 2000.

l. Fort Leonard Wood Command Policy #44-01, Network Access, Internet Use and Internet Monitoring.

2. Purpose. To provide consolidated guidance on the use and acquisition of portable electronic devices (PED) until an applicable regulation can be published by the DOIM.

3. Applicability and Scope.

a. Applies to all DoD personnel, contractors, and visitors that have access to FLW facilities, network, or information.

b. Applies to all wireless devices and technologies with data capabilities that operate as part of the enterprise network infrastructure, or any stand-alone wireless networks. This includes, but is not limited to commercial wireless networks and all PEDs, such as laptop computers, cellular/PCS devices, messaging devices, personal digital assistants (PDAs) and any other device capable of storing, processing, or transmitting information.

c. Does not apply to hearing aids, pacemakers, or other implanted medical devices, and personal life support systems.

4. Definitions. Terms used in this policy are defined in Enclosure 1.

5. Policy.

a. Wireless technologies, which include infrared, acoustic, and radio frequency, have the potential of introducing significant threats to FLW information systems. These threats are due, in part, to the unique vulnerabilities of the wireless extensions to the network located outside the physical confines of DoD controlled areas. The DOIM will thereforemanage and apply the following minimum requirements for use of wireless devices, services, and technologies of UNCLASSIFIED information:

(1) Identification and Authentication (I&A). Strong authentication and personal identification is required for access to all FLW information systems in accordance with DoD PKI policy (reference f) and AR 380-19 (reference g). I&A measures shall be implemented on all PEDs at the device and network level.

(2) Confidentially and Security. DA requires encryption of UNCLASSIFIED information for transmission to and from wireless devices. Accordingly, the FLW DOIM will utilize a standard, software based encryption program. Encryption is executed automatically when sending and receiving data messages through the FLW Campus Area Network (CAN), and is not currently required for voice messaging unless used to access a voice recognition/synthesis driven data application.

(3) Data Integrity. Wireless devices that store and process information often do not have the same degree of protection afforded by standard desktop operating and file management systems. All PEDs shall have protection measures in place according to the level required for the data stored (i.e. privacy act data shall be protected in accordance with DoD Directive 5400.11-R).

(4) Availability. Wireless devices are especially vulnerable to denial of service (DOS) attacks. The most common of DOS attack is the use of malicious code, which can be transmitted through synchronization, infrared beaming, and network access. Protective measures shall be taken to mitigate these risks and threats from outside the network, as well as potential interference from friendly sources.

(5) Synchronization. Synchronization is the most common means of exchanging data using PEDs. As with any exchange of data, there is the possibility of retrieving data that was not requested or authorized (i.e. malicious code). PEDs that are networked to the FLW CANshall not be synchronized with any system outside of the network.

(6) Antiviral Software. The use of DoD approved antivirus software on PEDs and workstations is mandatory. Antivirus software will be installed, activated, and virus signature files kept up-to-date on all PEDs that are connected to the FLW CAN. Any viruses detected must be reported to the unit Information Assurance Security Officer (IASO) immediately. If the IASO is not available, report the incident to the Information Assurance Manager (IAM).

(7) Infrared Beaming. Most PEDs, and some other devices such as printers and laptops, use infrared technology to communicate between devices within a close proximity (generally 4 to 36 inches). A program can deactivate the beaming notification, and then attempt to send itself out repeatedly, unknown to the user. Malicious code can be easily spread through infrared transfers on a PED because the default setting enables beaming. All PEDs will have the beaming feature disabled when not in use.

(8) Lost or Stolen PEDs. PEDs are easily lost or stolen. To protect against loss of sensitive information the use of DoD approved file/data store encryption software is mandatory. Encryption software for applicable PEDs can be obtained through the Directorate of Information Management (DOIM).

b. Wireless technologies/devices shall not be used for storing, processing, and/or transmitting CLASSIFIED information without the explicit approval of the Designated Approving Authority (DAA) in accordance with DoDD 5200.28 (reference c). Additionally, use of any DAA approved device shall meet all protection requirements in accordance with HQDA Ltr 25-02-1 (reference f).

c. Wireless devices shall not be operated inside a permanent, temporary, or mobile Sensitive Compartmented Information Facility (SCIF) in accordance with chapter 15 of Joint DoD/IIS Cryptologic SCI System Security Standards.

d. Wireless devices shall not be connected to the FLW CAN without the approval of the DAA. Contractor and privately owned PEDs shall not be connected to the FLW CAN or any government automation equipment (whether the device is connected or disconnected to the CAN) without explicit approval by the DAA. Contractor and privately owned PEDs will be evaluated on a caseby-case basis for approval and must meet all risk mitigation and accreditation requirements prior to consideration.

(1) All expenses to meet these requirements shal be incurred by the owner for privately owned PEDs. Expenses for contractor owned PEDs shall be determined by the contract in place.

(2) Contractors, licensees, private PED owners, and any other non-government PED individual users who desire access will sign a user agreement before access is granted, accepting and acknowledging primary responsibility for any damage caused to the FLW network and waiving any claim for damage which might occur to the private PED resulting from the connection.

e. Acquisition of PEDs and supported software shall be the responsibility of the FLW DOIM.

(1) All PED hardware, software and services standardization will be determined by the DOIM.

(2) Organizations requiring PEDs shall submit a capabilities request (CAPR) for automation equipment in accordance with current procurement and acquisition policies.

(3) MANSCEN funds will only be used to purchase PEDs (excluding laptop devices), software, or services for personnel in O-6 and above positions.

(a) Approval by an O-6 or above will be required for the purchase of PEDs (excluding laptop devices), software, or services for personnel in O-5 and below positions.

(b) Funding of PEDs (excluding laptop devices), software, or services for personnel in O-5 and below positions will be from other than MANSCEN funds. Funding includes any and all reoccurring costs for the device, software, and service.

(4) Purchase of any PED, software, or service with government funds is prohibited by the organization without explicit approval from the DOIM.

6. Acknowledgement. Each activity commander/director shall ensure all FLW personnel using PEDs understand the policy.

7. Enforcement. This policy is a lawful general order and as such violations of it are punishable under the Uniform Code of Military Justice (UCMJ). It is authority for taking adverse personnel action against DoD civilian personnel. Contractors not adhering to this policy shall face loss of access to the FLW information infrastructure. Intentional and significant violations of this policy may result in the violator being held financially liable for the cost of improper use.

8. Proponent. The proponent for this policy is the DOIM, 563-6113

R. L. VAN ANTWERP
Major General, USA
Commanding

Enclosure
as

DISTRIBUTION:
All Brigades, Battalions, Companies,
Detachments, Tenant Units, Directorates
Personal Staff Offices, and Contractors

Definitions

Assured Channel. A network communication link that is protected by a security protocol providing authentication, confidentiality and data integrity, and employs US Government approved cryptographic technologies whenever cryptographic means are utilized.

Designated Approving Authority (DAA). The official designated by the local commander, which has the power to decide on accepting the security safeguards proscribed for an information system. The FLW DAA is the Director of the DOIM.

End-to-End. Automated Information System from the user device up to the security border of the FLW network.

Identification & Authentication (I&A). The process of accepting a claimed identity and establishing the validity of that claimed identity.

Portable Electronic Device (PED). Any non-stationary electronic device with capability of recording, storing, and/or transmitting information. This definition includes, but not limited to personal digital assistants, cellular/PCS phones, two-way pagers, e-mal devices, and hand held/laptop computers.

Wireless. Technology that permits the transfer of information (passive or active) between separate points without physical connection.